Sentinel

Software User Manual

for the range of Ringdale Network I.D. Readers

Connecting people and information

RINGDALE

Version 3.2 April 2002

COPYRIGHT

Copyright 2002 © Ringdale UK Ltd. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or any computer language, in any form or by any third party, without prior permission of Ringdale UK Limited.

DISCLAIMER

Ringdale UK Ltd. reserves the right to revise this publication and to make changes from time to time to the contents hereof without obligation to notify any person or organisation of such revision or changes. Ringdale UK Ltd. has endeavoured to ensure that the information in this publication is correct, but will not accept liability for any error or omission.

Because of the fast pace of software development it is possible that there will be minor differences between the manual and the program.

TRADEMARKS

All trademarks are hereby acknowledged.

Contents

Introduction **5**

Sentinel Installation **6**

First Time Set-Up Procedure **8**

Configuring an ID Reader/Access Controller to the Network **12**
Deleting an ID Reader/Access Controller From Sentinel 16

Setting Up Users for the ID Reader **17**
Editing and Removing Users 20

Access and Security Settings **21**
Access Times 22
Calendar 24

Assigning Users to a Group and Managing Users for More than One ID Reader **26**

Fingerprint Reader Option **30**
Creating Reports for a Fingerprint Reader 42

Uploading Settings to the ID Reader/Access Controller **44**

Door Strike and Bolt Control Options **50**

Time and Attendance Terminal **54**

Retrieving Information from the ID Reader/Access Controller **55**
Automatic Log Retrieval 55
Manual Log Retrieval 57
Viewing a Log 58
Flag Codes 59

(Cont)

Creating Reports **60**
Access Logs 60
Groups and Users 63
User Information 64
Printing and Exporting Reports 66

Personnel Monitor Option **67**
Adding a Photograph to a User's Details 67
Setting Up Sentinel on the Monitor PC 68
Starting the Sentinel Monitor 69
Associating the Monitor to an ID Reader/Access Controller 70

Uninstalling the Sentinel Software **73**

Introduction

Sentinel is Ringdale's management software for use with their access control systems and Network I.D. Readers. Sentinel can be installed on any Windows 95/98/ME/NT4/2000 PC connected to an Ethernet Local or Wide Area Network (LAN or WAN).

It provides full configuration, management and monitoring capability for applications such as door strikes, bolts, and time & attendance systems across the network from the administrators PC.

Issue each employee with an ID card, pin number (or even fingerprint recognition can be used if required) that has a unique built-in code that can identify them. Once the user has been identified they can be granted access through a door, clocked in etc. depending on the application for which the ID reader is being used.

The Sentinel software is used to configure the ID reader or access controller to the network and to set up users. Sentinel allows comprehensive access and security settings to be configured for each user, and the creation of log and database files for generating reports of usage. Sentinel can manage multiple readers/controllers on the network.

The ID reader/controller downloads its data to the PC running Sentinel once every minute, ensuring that the software always has an up-to-date record.

Setting up the ID reader/access controller involves two main procedures:

1 Installing the ID reader/access controller in suitable locations.

2 Installing and configuring the software onto the designated PC.

This guide provides installation, configuration and user instructions for the Sentinel software and should be used in conjunction with the ID reader or access controller *Quick Installation Guide* also supplied.

Sentinel Installation

The Sentinel software is found on the CD enclosed with the pack. Install the software on the PC that you want to use as the server. This can be any networked Windows 95/98/ME/NT4/ 2000 PC. It is recommended that if installing a new version of Sentinel the old version should be uninstalled first.

Important: once installation is complete it is necessary to reboot the PC before using the software. For uninstallation instructions see the section *Uninstalling Sentinel* in this guide.

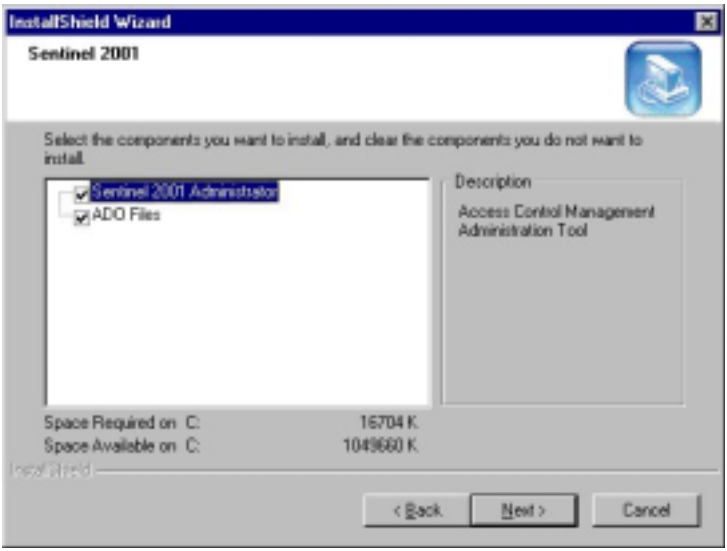
Use the following procedure to install the software:

1 Load the CD into the PCs CD drive.

2 Use *Windows Explorer* to browse the CD and select the **Software** directory.

3 Open **Sentinel 2001.exe**.

4 Follow the on screen instructions until the window displayed below appears:



Ensure that both options in this window are ticked.

5 Click **Next** and follow the on screen instructions to complete the installation.

6 Reboot the PC.

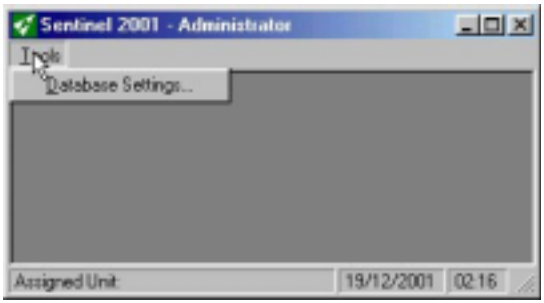
First Time Set-Up Procedure

The following procedure ***Must*** be completed before attempting to use the Sentinel software for the first time

1 After the installation and reboot are complete, open the Sentinel software using the following path:

Start/Programs/Ringdale/Sentinel 2001/Sentinel 2001

The following window will be displayed (note: the window may appear slightly different to this):

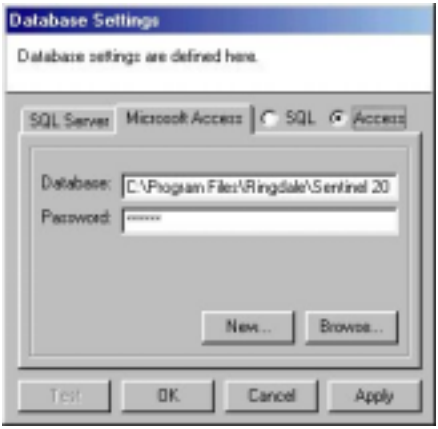


2 From the **Tools** menu select **Database Settings**.

It is necessary to connect the program to the database that is to be used for Sentinel. The most commonly used database is Microsoft Access, but for environments where a large amount of information is generated there is the option to connect to a more powerful SQL Server. Select either *Microsoft Access* or *SQL Server* as required:

Microsoft Access

i Click the **Access** radio button and then click on the **Microsoft Access** tab to display the page shown following (**note:** the PC running the Sentinel software does not need to have *Access* installed, Sentinel can be associated to an Access database on another networked PC if required):



ii Click on the **New** button to display the **Create Access Database** window and in the **File Name** field enter a name for the database:

(Suggested): **Sentinel 2001.mdb.**

Navigate to the directory where the database is to be located - if *Access* is installed on the Sentinel PC itself it is recommended that the database be kept with the other program files in:

C:\Program Files\Ringdale\Sentinel 2001

Important: ***If more than one copy of Sentinel is installed on the network (that will share the management of the same ID readers/access controllers) it is recommended that the Access file be put in a location where it can be shared by all copies of the software that are used (all other installations should point to the same location).***

Click the **Save** button and the path will appear in the *Database* field as shown above.

iii Enter a **Password** to restrict access to the database.

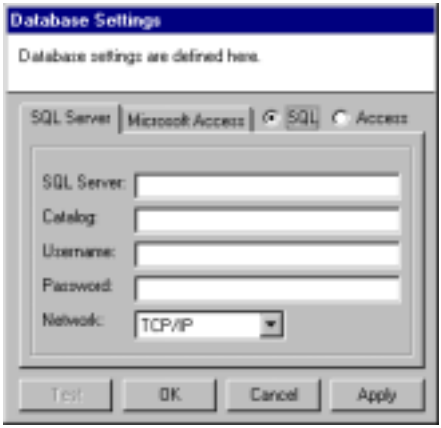
iv Click the **Apply** Button, then click the **Test** button. A dialog box will ask if the tables for the database should be created. Click the **Yes** button.

Note: A dialog box might ask if the new settings should be used. Click **Yes** again.

v The message *Passed - Connected to Database* will be displayed (the connection can be checked at any time by clicking the *Test* button). Click **OK** to exit the *Database Settings* window.

SQL Server

i Click the **SQL** radio button and then click on the **SQL Server** tab to display the page shown following:



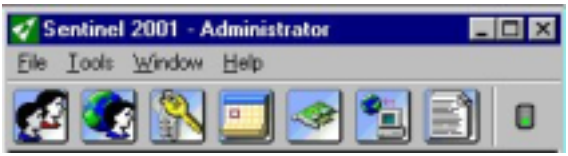
ii Enter the SQL details into the relevant fields (this information will be supplied by your SQL/Database administrator).

iii Click the **Apply** Button, then click the **Test** button.

iv A dialog box will ask if the new settings should be used. Click **Yes** again.

v The message *Passed - Connected to Database* will be displayed (the connection can be checked at any time by clicking the *Test* button). Click **OK** to exit the *Database Settings* window.

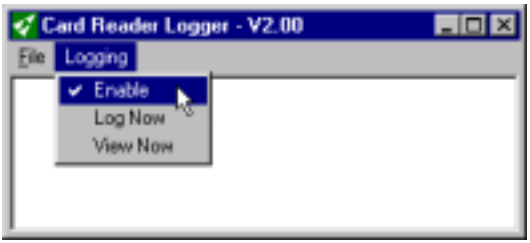
3 The Sentinel main window should now display a full set of menu and icon options similar to the example shown below (if not, check that the database configurations are correct as detailed previously):



These options are used to configure and manage the ID reader/ access controller and will be discussed later in the manual.

4 Optional
If the automatic download option is to be used to retrieve the log from a device (see the chapters *Retrieving Information from the ID Reader/Access Controller* and *Creating Reports* for full details) the logging facility will need to be enabled.

Double click on the **Ringdale** icon located in the bottom right corner of the screen, as shown here. This will display the Sentinel Logger window as shown below:



From the Logging drop-down menu, ensure that the Enable option is ticked. Minimize the Logger window.

This completes the *First Time Set-Up Procedure*. Proceed to the next chapter *Configuring an ID Reader/Access Controller to the Network*.

Configuring an ID Reader/ Access Controller to the Network

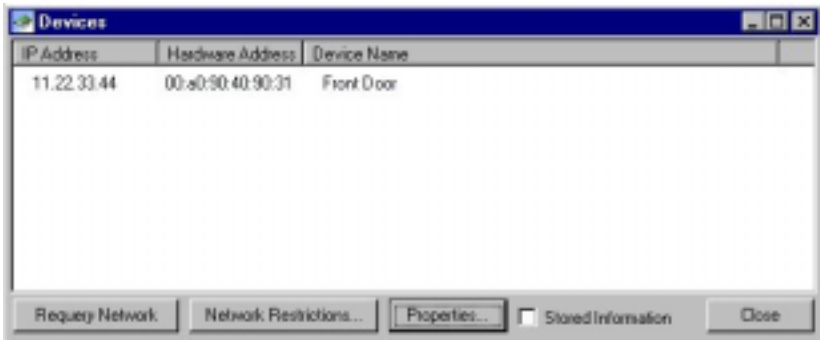
To configure an ID reader/access controller to the network use the following procedure:

Open the Sentinel program by selecting the following path from the **Start** menu:

Programs/Ringdale/Sentinel 2001/Sentinel 2001

The Sentinel main window will be displayed.

1 Click on the **Devices** icon at the top of the window, as shown here. The following window will be displayed (**note:** this will be empty when opened for the first time):



2 After ensuring that the ID reader/controller has been installed on the network, click the **Requery Network** button. All ID readers/controllers on the network will be listed in the window. Sentinel will display the details of the device to be configured with a factory default IP address of:

11.22.33.44

Important: If installing more than one ID reader/access controller it is advised that each is configured immediately after installation before the next is installed onto the network. There

will be difficulties in identifying which device is which if more than one unconfigured device is on the network sharing the same factory default IP address.

Locating ID Readers/Access Controllers on Different Networks/Subnets

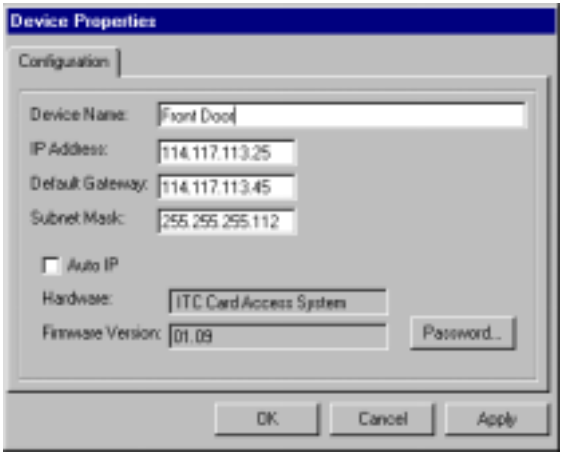
If the ID reader/access controller is on a different network/ subnet to the PC with the Sentinel software it will not be instantly identified by the program. Click on the **Network Restrictions** button to display the following dialog box:

Click on the **Add** button to display this dialog box.

Use the subnet address or the IP Address of the device (xxx.xxx.xxx.255 will find all devices on the network without having to enter a specific IP address) and click **OK**. The address will appear on the list in the *Network Restrictions* dialog box. Ensure that the address is selected before clicking the **OK** button again.

Click the *Requery Network* button to list the device in the *Devices* window.

3 Highlight the device on the list and click the **Properties** button to display the configuration page as shown following:



Use this page to configure the ID reader/controller to the network by providing the **Device Name** (this should be something that will easily allow the specific device to be identified), **IP Address** and **Subnet Mask**.

If the PC and the device are on different networks, it will be necessary to enter the **Default Gateway IP Address** as well.

Tick the **Auto IP** check box to allow the IP address of the device to be set using *Ping* or *arp*. ***This feature is not activated by default as it can create a potential security risk and should only be used if specifically needed*** (this is ***Not*** a DHCP option).

Because of the sensitive nature of the information that is configured with this software, access to change any of the settings can be restricted by setting a password.

Click the **Password** button and enter a password into the **New Password** box. Type in the confirmation and click on **OK**.

Note: It is recommended that all devices be set with the same password - while different passwords for different devices can be used with manual retrieval of logs, if the automatic download option is used to retrieve the device logs only ***One*** password must be set for all devices.

Access to change any of the settings in the software will now be restricted to those who have the password.

Click **OK** or **Apply** to apply the settings.

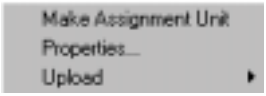
Once this is done, give Sentinel a few seconds to re-initialise itself internally and then click the **Requery Network** button in the *Devices* window. This will refresh the list with the updated information.

Additional Options

Other features available in this window include

Stored Information
Ticking this box will make available the stored information that Sentinel has about each device. This would mean, for example, that if a device had lost its connection to the network the last available information from the device would be displayed rather than the device not being displayed at all.

Right Click Options
Right clicking over a device on the list will display the following pop-up window:



The **Make Assignment Unit** option should be selected for the device that will be used to set up the users on Sentinel if the fingerprint reader option is being used or ID cards with 'hidden' coded numbers are being used. See the chapters *Setting Up Users for the ID Reader* and *Fingerprint Reader Option* for more details on this.

The **Properties** option provides an alternative method of opening the *Device Properties* window instead of clicking the *Edit* button.

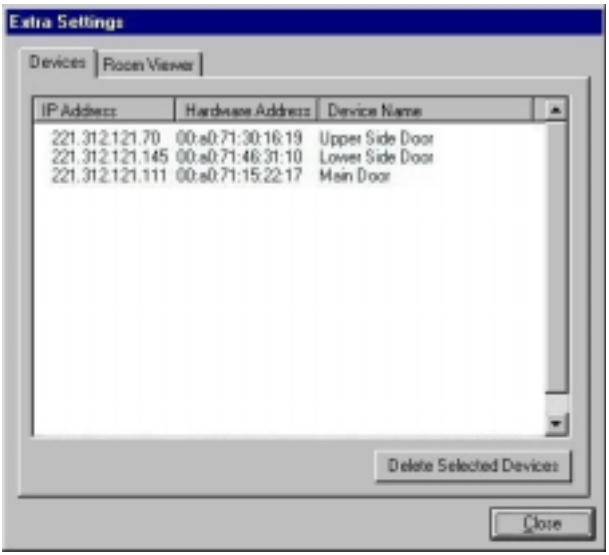
Any changes made to the *Calendar*, *Access* or *Groups* information must be uploaded to the device/s to take effect. The **Upload** option provides a quick method to do this. See the chapter *Uploading Settings to the ID Reader/Access Controller* for full details of this feature.

The device is now configured to the network. Proceed to the next chapter, *Setting Up Users for the ID Reader*.

Deleting an ID Reader/Access Controller From Sentinel

If an ID reader/access controller is taken off the network, it will still be listed in Sentinel unless it is deleted. Use the following procedure to remove a device from Sentinel:

1 In the Sentinel main window, select the **Extra Settings** option from the **Tools** menu. The following window will be displayed (the **Devices** page should be shown by default - if it isn't click on the tab to display it):



2 The page will list all the ID readers/access controllers that have been configured by Sentinel. Select the device to be removed.

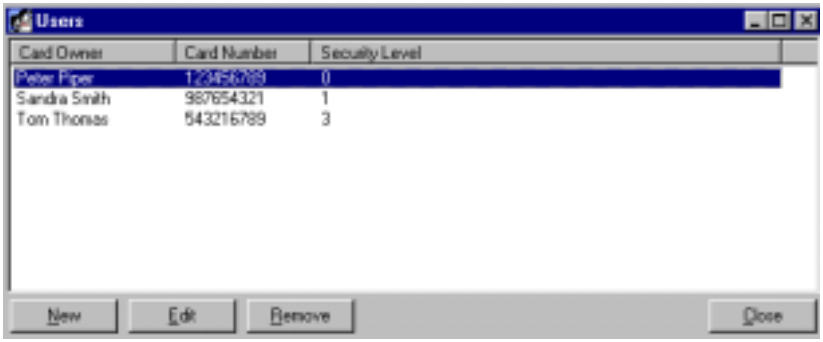
To select multiple users hold down the **Control** key while selecting, or to select a block of users together hold down the **Shift** key and select the users at the top and bottom of the block.

Click the **Delete Selected Devices** button and the device/s will be removed from Sentinel. Click the **Close** button to exit.

Setting Up Users for the ID Reader

To set up users for the ID reader, proceed as follows (**note:** if using the *Fingerprint Reader Option* see also the separate chapter related to this later in the manual).

1 In the Sentinel main window, click on the **Users** icon, as shown here. The following window will be displayed (**note:** this picture shows the window with users already configured - on first time set-up this window will normally be empty:



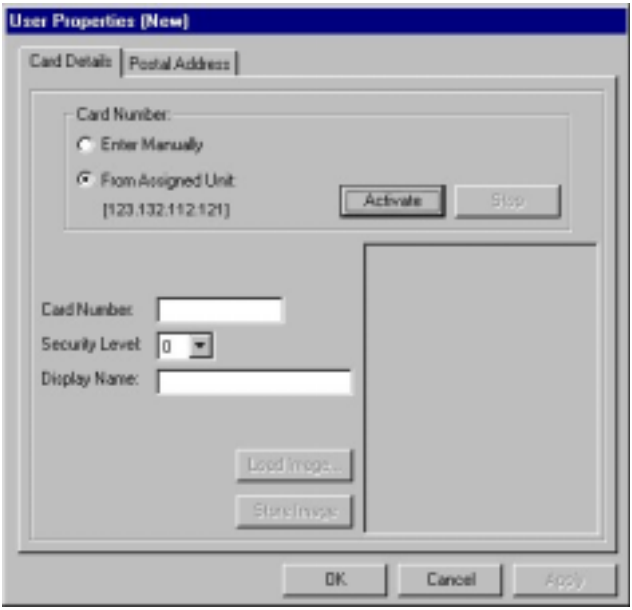
2 To set up a new user click the **New** button to display the *User Properties* window (an example is shown on the following page). Ensure that the **Card Details** tab is selected:

Note: Sentinel provides the option to load and store a photograph of the user if required - the system works perfectly well whether this option is used or not.

If the *Personnel Monitor Option* is installed, it is advised that photographs be used to get the most out of the system - see the separate chapter later in the manual for full details on this feature.

3 In the **Display Name** field, enter the name of the user.

4 The next step depends on the type of ID reader that is being used. Select the relevant procedure from the options (i), (ii) or (iii).



(i) ID Card Reader with Coded Cards (Pre-Assigned Numbers)

For a card reader with coded cards (where each card contains its own unique 'hidden' number) ensure that the **From Assigned Unit** option is selected in the *Card Number* field as the number will be automatically entered into Sentinel.

Ensure that the assignment unit displayed is the one to be used for reading the cards for registration- to select the required reader/access controller click the *Device* icon in the Sentinel main window and right-click over the device's IP address. From the drop-down menu select *Make Assignment Unit*. This will display the unit's IP address on the *Card Details* page displayed previously.

Click the **Activate** button. Once this button is activated, present the user's ID card to the card reader. **Note:** this must be done within 10 seconds.

The number of the card will appear in the **Card Number** box.

(ii) ID Card Reader with Manual Number Entry / Key Pad Pin Number Entry

If the number of the user's card is known it can be entered manually. If the key pad option is being used the pin number for the user must be entered manually.

Ensure that the **Enter Manually** option is selected in the *Card Number* field.

Enter the ID number into the **Card Number** box (maximum of ten characters).

(iii) Fingerprint Reader

See the *Fingerprint Reader Option* chapter later in the manual.

5 From the **Security Level** drop-down list select the security level required for this user.

Note: Sentinel has up to sixteen different levels that can be set (it is not necessary to use all sixteen). See the following chapter *Access and Security Settings* for details on security level configuration.

6 If a photograph of the user is required, click the **Load Image** button and browse to the location of the file. Click **OK** and the photo will be displayed in the image box. If the photo is correct click the **Store Image** button to store the photo in the database.

The photo can be viewed at any time by opening the *User Properties* window.

7 Clicking the **Postal Address** tab allows for more comprehensive information on the user to be entered on the displayed page if required. This is an optional feature.

8 Click **OK** to close the *User Properties* window, saving all the information that has been entered. The user will appear on the list in the *Users* window.

Repeat the procedure for as many users as required.

Important Note

This procedure has set up a user within Sentinel but before their ID can operate the user has to be associated to at least one group, and that group will need to be associated with at least one ID reader/controller device. This information has to be uploaded to the specific device/s required. Please see the following chapters of this manual before attempting use.

Editing and Removing Users

To change the details of an existing user, highlight the user in the list in the *Users* window and click on the **Edit** button. Change the details as required and click **OK**. The details will be amended.

To delete an existing user from Sentinel, highlight the user in the list of the *Users* window and click on the **Remove** button.

Access and Security Settings

Sentinel has a sophisticated access and security setup to allow a high level of management for all users of the ID readers. If all users can have full access 24 hours a day, seven days a week, then these features need not be configured, otherwise use the following to set up access restrictions for users.

Each user is assigned a security level (see previous chapter *Setting Up Users for the ID Reader* for details on how to assign a security level to a user) through which the hours and the days that the user can gain access are set.

Following is a simple example to demonstrate how the system works:

Company A uses only two of the available day types:

Day Type 0 is for weekdays (this is the default day type)
Day Type 1 is for weekends

They use only three of the available security levels:

Level 2 is used for general employees
Level 1 is used for managers
Level 0 is used for directors (this is the default level type)

On weekdays (day type 0), general employees with their security level set at 2 can use the ID reader only between the hours of 08.00 and 19.00.

On weekends (day type 1), they are prevented from using the ID reader at all.

On weekdays, managers with their security level set at 1 can use the ID reader only between the hours of 08.00 and 21.00.

On weekends, they can use the ID reader only between 09.00 and 17.00.

Directors, with their security level set at 0 have 24 hour access for both day types (this is the default setting for level 0).

With up to 16 security levels available and up to eight different day types that can be set, the program allows great flexibility for configuring the users to suit any variety of requirements.

In addition, for situations where more than one ID reader is being used, the *Groups* feature allows the list of users to be divided into groups. Each group can then be assigned to a particular ID reader (see the following chapter *Managing Users for More than One Reader* for full details on this facility).

Configuring the access and security settings involves two main procedures which are detailed following, ***these must be completed for all set-ups*** unless all users are to have access 24 hours a day, seven days a week.

a) Access Times

1 In the Sentinel main window, click on the **Access Times** icon, as shown here. The following window will be displayed:

2 From the **Day Type** drop-down list, select the day type that you want to configure (there are 8 distinct day types – each day type represents a 24 hour time period).

3 In the centre of the window is the security levels display – 16 rows representing the access levels, with each row representing a 24 hour time period.

To set the access time for each security level, move the cursor over the display, hold down the left mouse button and drag to fill the security level as required.

Above the display, two boxes will show the **Start** and **End** of the access time that is being selected (note: it's easiest to drag down and to the right). The **Cursor** box allows continuous monitoring of the time where the cursor is located. The smallest individual time period for which access can be granted is 15 minutes.

4 When you have selected the time period required, click the **Allow** button. A blue bar shows where the access time has been set.

5 Repeat the procedure to set up the access time for as many security levels as required.

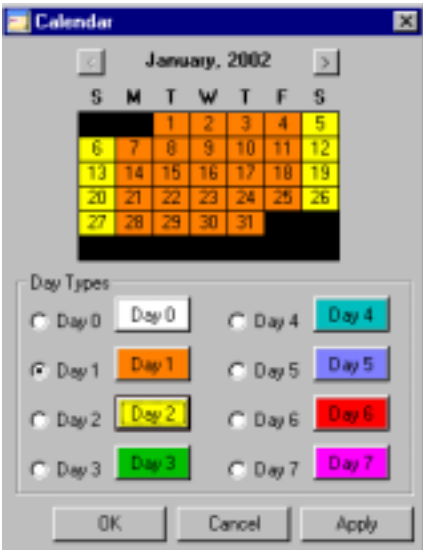
Note: It is not necessary to use all security levels. It is recommended that a 24 hour security level is created and that *level 0* is used for this.

To remove or change the configuration of a security level, select the required level and then click the **Disallow** button. This will remove the setting.

Repeat the procedure for as many day types as required. Click **OK** to exit the window keeping the changes you have made.

2) Calendar

1 In the Sentinel main window, click on the **Calendar** icon, as shown here. The following window will be displayed:



Having set up the access settings for each security level of each day type in section 1, it is now necessary to configure each day type to the calendar for Sentinel to know when each user can and cannot use their card.

2 At the top of the window is a text box indicating the current month and year on display. To step forward a month, click on the button with the arrow pointing to the right. To step back a month, click on the button with the arrow pointing to the left (note: you cannot go back beyond the current date).

Find the dates for which access configuration is required.

3 At the bottom of the window is a colour coded list of the day types. There are two different methods for selecting the day type for the calendar.

One is suitable for quickly setting large blocks of days - for example if all weekdays are to be of the same day type.

The other allows quick setting of single days - for example if a national holiday (with a different day type) needs to be set within a large block of the normal working day type.

By holding down the left mouse click and dragging, a box can be drawn around a block of days. Click on the **Coloured** button for the day type required - for example if all weekdays are to be set at day type 1, after the block of days has been drawn on the calendar, click the orange *Day 1* button. All days within the block will become orange and are now set to that day type.

By clicking the **Radio** button beside the day type and then double clicking on a single day within the calendar, that day can be individually set to the required day type - for example if the first Monday of the month is a national holiday with its own day type (for instance type 3), click the radio button beside *Day 3* and then double click that Monday on the calendar and it will be coloured and set to the required day type.

4 Repeat the procedure for as many day types as required. When the month is configured to your requirements, move to the next month to be configured.

Important

Any days on the calendar that do not have a day type assigned to them will default to day type 0.

Click the **Apply** button to ensure the settings are saved.

5 When the calendar has been fully configured as required, Click **OK** to exit the window. The configurations that have been set will be saved (to exit the window without saving the settings click **Cancel**).

The ID reader access and security configuration is now complete.

Note: before the ID reader can use these settings they must be uploaded to the device/s (see the chapter *Uploading Settings to the ID Reader/Access Controller* for details of this procedure).

Assigning Users to a Group and Managing Users for More than One ID Reader

For situations where more than one ID reader is being used on the network, Sentinel provides a group management feature. This allows the list of users to be divided into groups. Each group can then be assigned to a particular ID reader or readers as required.

A simple example of this feature in operation would be:

Company B has two ID readers.

Reader 1 is for the main entrance
Reader 2 is for access to the accounts office

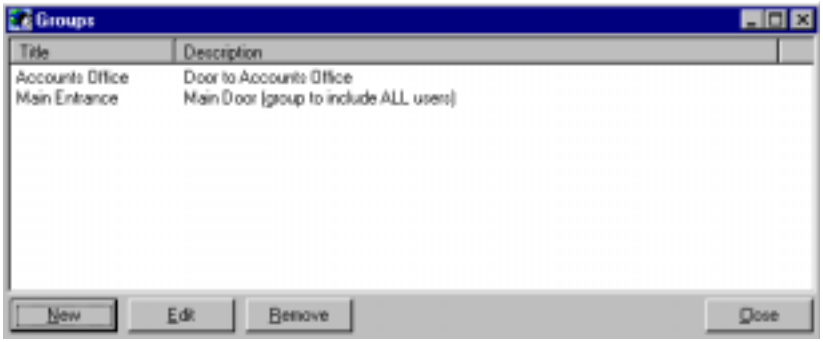
All employees require entry through the main door.
Only accounts employees have entry to the accounts office.

All users are assigned to reader 1

A group is created in Sentinel for accounts employees. This group is then assigned to reader 2. Only employees in this group can access the accounts office.

Use the following procedure to create a group and assign the group to the required ID reader.

1 In the Sentinel main window, click on the **Groups** icon, as shown here. The following window will be displayed:



This window will display a list of all user groups that have been set up in Sentinel (note: this window will be empty when setting up user groups for the first time).

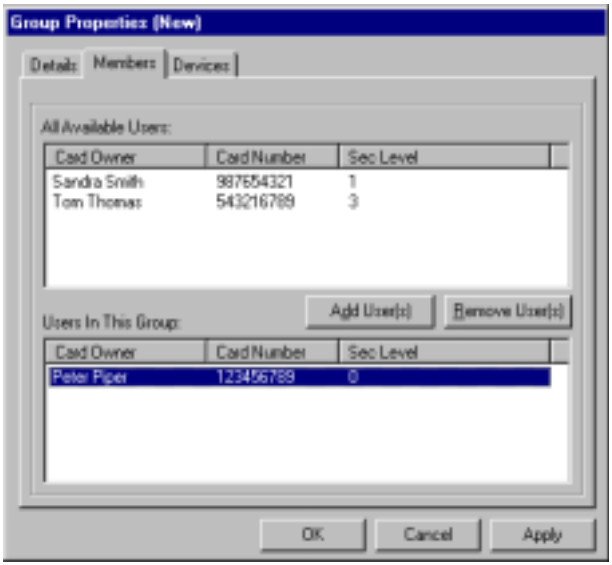
Important

ALL users must be included in at least one group

In the example shown all users are included in the group for the main door but it is not necessary to create a group specifically for all users (though this does ensure that no user gets missed).

2 Click on the **New** button to display the **Details** page of the **Group Properties** window. Enter a **Title** for the group and then enter a brief description of the group into the **Description** field (maximum 50 characters).

3 Click on the **Members** tab to display the following page:



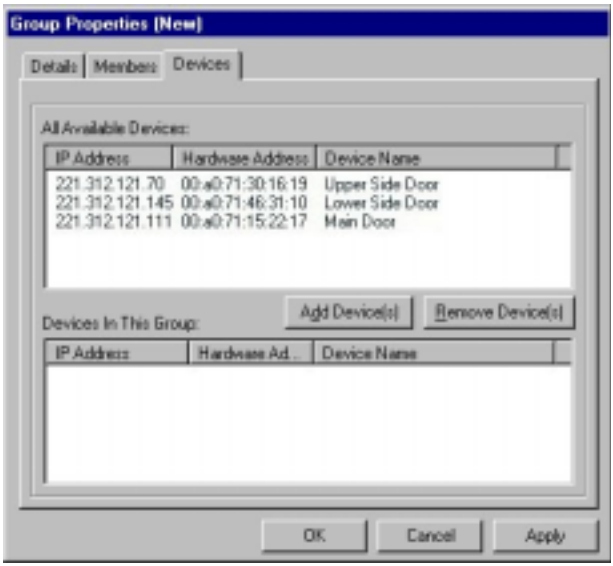
In the **All Available Users** field will be listed all the users that have been set up within Sentinel. Select a user or users that are to be members of the group from this field.

To select multiple users hold down the **Control** key while selecting, or to select a block of users together hold down the **Shift** key and select the users at the top and bottom of the block.

Click the **Add User(s)** button and the selected user/s will be moved into the **Users in This Group** field. Repeat the procedure until all users required for this group are in the lower field.

If a user or users need to be removed from the group list, select them following the same method as above but in the lower field. Click the **Remove User(s)** button and the users will be moved back to the top list.

4 Click on the **Devices** tab to display the following page:



On this page, assign a specific ID reader or readers to the group. In the **All Available Devices** field will be listed all the ID readers/access controllers that have been set up within Sentinel. Select a device or devices that are to be associated with this group from this field.

To select multiple devices hold down the **Control** key while selecting, or to select a block of devices together hold down the **Shift** key and select the devices at the top and bottom of the block.

Click the **Add Device(s)** button and the selected device/s will be moved into the **Devices in This Group** field.

If a device needs to be removed from the group list, select it following the same method as above but in the lower field. Click the **Remove Device(s)** button and the device will be moved back to the top field.

5 Click **OK** to exit the window saving the settings. The new group will be listed in the *Groups* window.

Repeat procedure to set up as many groups as required.

Changing Group Configurations

To make changes to a group set-up, select the group from the list displayed in the *Groups* window and click the **Edit** button.

The *Group Properties* window will be displayed with the three pages *Details*, *Members* and *Devices*. To alter the set-up follow the same instructions as previously described in this chapter. Change, add and remove users and devices as required.

Click **OK** to exit the window saving the changes.

Deleting Groups

To delete a group from the *Groups* List, select the group and click on the **Remove** button. The group will be removed.

Important Note

Any changes made to a group set-up must be uploaded to the relevant device/s (see chapter *Uploading Settings to the ID Reader/Access Controller*).

Fingerprint Reader Option

If a fingerprint reader is being used in conjunction with Sentinel the procedure for creating users is different.

Important Information

When using the fingerprint reader option please bear the following in mind:

a) Care needs to be taken when setting up users for the fingerprint reader. The more meticulous the approach taken with this procedure the clearer and sharper the image will be. The stronger the quality of data that is stored by Sentinel the more reliable and consistent will be the access capability of the user (the actual fingerprint is not stored by Sentinel, only points of reference from it). Below are some tips to help achieve this:

- **i** Ensure the fingerprint sensor is clean (use a soft, dry cloth) before starting and that it is regularly wiped (especially if users have particularly oily hands).
- **ii** Users should wash and dry their hands prior to the start of the procedure.
- **iii** The fingerprint should cover as much of the sensor as possible. Place finger directly on the sensor without sliding across the surface. Repeat the action until the administrator believes optimal finger placement has been achieved.

b) It is recommended that each individual registers two or three fingers. There will then be a backup print that can be used in the event of one of the fingerprints becomes temporarily or permanently altered (for example by a paper cut or minor burn).

c) It is useful to have the fingerprint reader close to the PC running the Sentinel software when setting up new users.

d) Every finger registered will need to be processed four times to ensure a thorough identification is possible.

Setting Up Users for a Fingerprint Reader

When registering users for a fingerprint reader either the Sentinel Service needs to be stopped or the server port for the fingerprint controller needs to be changed. Which option is preferred will depend on the set-up of the access control system.

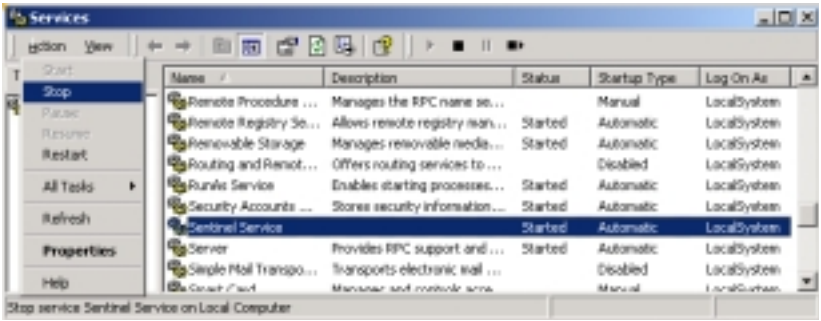
Stopping the Sentinel Service

The Sentinel Service runs in the background and is automatically activated during installation. If this method is used, when the service is stopped the access control system will be inoperative, thus new users cannot be added at the same time as existing users need access through doors or to clock in/out etc. This is most suitable for small installations, the more readers/controllers that are on the system, the more impractical this method becomes.

How the service is stopped will depend on the version of Windows the PC is running.

2000

From the **Start** menu select **Settings/Control Panel/ Administrative Tools/Services** to display the following window:



Select **Sentinel Service** from the list and click the **Action** button in the top left corner of the window. Select **Stop**. On the list, the status of the service will no longer be listed as *Started*.

NT4 +
From the **Start** menu select **Settings/Control Panel/Services**. Select **Sentinel Service** from the list and click the **Stop** button. On the list, the status of the service will no longer be listed as *Started*.

95/98/ME
Because these platforms do not run a *Services* feature the service is run as an executable program. To stop the service running press **Control**, **Alt** and **Delete** together ***Once*** to display the *Task Manager*. Select **Sentinelservice** from the list and click the **End Task** button. The service will be stopped.

Changing the Server Port

Sentinel provides the ability to change the server port to allow new users to be registered without stopping the Sentinel Service. This enables the access control system to continue to operate so access can be maintained at all times.

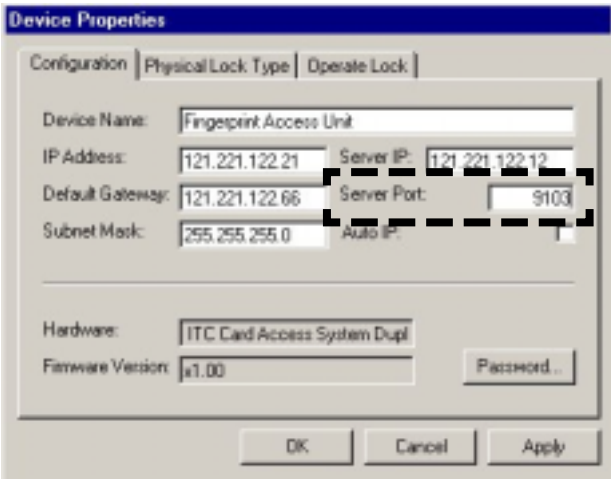
If there is a desktop fingerprint reader/controller that is dedicated to administration and new user set-up only (therefore doesn't directly manage a door or a time and attendance terminal), then this controller can be set to this port permanently to permit easy registration.

If a fingerprint reader/controller that is managing a door or time and attendance terminal needs to be 'commandeered' for the registration of new users then changing the port will prevent that particular device from being used for access control, but because the Sentinel Service is still operating, all other reader/controllers on the network can still function normally. **Important:** In this situation the server port will need to be changed back to the default setting when the user registration has been completed, allowing the reader/controller access control function to operate again.

Use the following procedure to change the server port:

1 Click on the **Devices** icon at the top of the Sentinel software main window.

2 From the list of available devices select the controller required and click the **Properties** button to display the following window:



Fingerprint reader controllers will have an additional feature visible on the **Configuration page** - ***Server Port*** - as shown above.

Note: If this feature is not present then the firmware on the device will need to be upgraded - please contact Ringdale technical support for this (contact details on the back cover of the manual).

The default setting is Server Port 9103

3 Change the server port to another convenient port (suggested 9104, providing this is not already in use - check with the network administrator for this information).

4 Click **OK** to save the change and exit the window.

Once either the Sentinel Service is stopped or the server port has been changed, Sentinel is ready to set up new users for the fingerprint reader.

Registering a New User for a Fingerprint Reader

1 In the Sentinel main window, click on the **Users** icon to display the *Users* window. Click on the **New** button to display the *User Properties* window for a new user.

2 Ensure the *Card Details* page is displayed and in the *Card Number* field select the **Enter Manually** option.

3 Enter the user's name into the **Display Name** field and select a **Security Level** from the drop-down box (Sentinel has up to sixteen different levels that can be set - it is not necessary to use all sixteen - see the following chapter *Access and Security Settings* for details on security level configuration).

4 Click the **Apply** button and an extra tab option will appear in the *User Properties* window - **Fingerprints**. Click this option to display the *Fingerprints* page shown below:

5 (This step is only applicable if the *Changing the Server Port* method is being used - if the Sentinel Service has been stopped instead proceed to step 8)

In the bottom right corner of the page is the server **Port** button (default setting 9103). Click the button to display the text box and button shown here.

Change the server port to match that previously set on the *Device Configuration* page (suggested 9104). Click the **Set** button and the new port will now be displayed on the button.

6 Click on the radio button for the first finger that is to be registered.

7 Click on the **Listen** button and ask the user to apply the correct finger to the sensor of the fingerprint reader. After a few seconds the fingerprint will be displayed on the Fingerprint Page as shown in the example below:

It is important to get as clean an image of the fingerprint as possible. Don't be afraid to redo the fingerprint if the image displayed is poor. The better the data held for each finger by Sentinel the more reliable will be the recognition by the reader in everyday use.

Don't forget to employ the tips detailed at the start of this chapter to achieve consistent results of a high standard.

8 Two buttons will now be enabled - *Verify* and *Stage 1*:

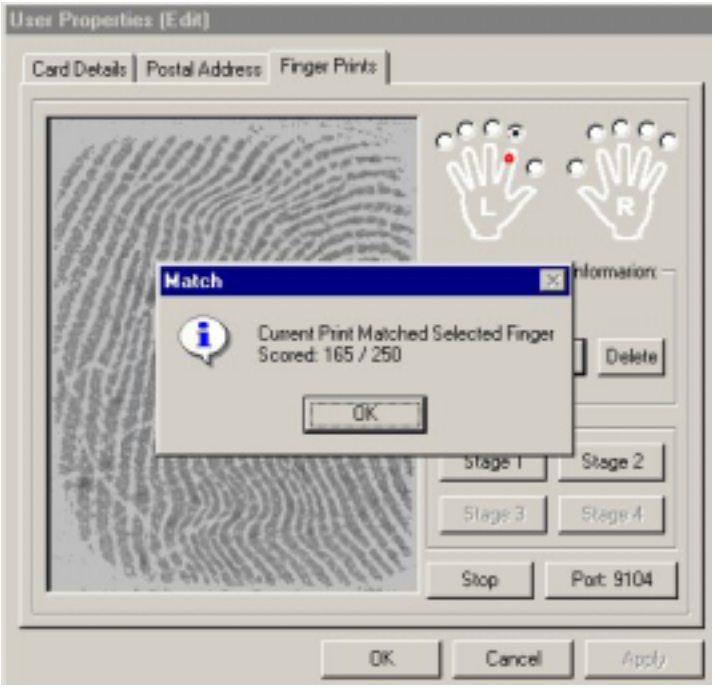
Click the **Verify** button. This allows the print to be verified to ensure that it does not match too closely an existing print in the database. In the very unlikely event that it does ask the user to select another finger for registration. After the *Verify* button has been clicked the following will be displayed:

Click **OK** and if happy with the fingerprint click the **Stage 1** button to hold this print as the first of the four that is needed for ***each finger*** that is to be registered.

If the print is accepted the *Stage 2* button will become available.

Note: Each stage requires the user to provide a new fingerprint of the ***Same*** finger which will be matched to the original - this is to allow Sentinel to learn to recognize the fingerprint. A red dot will appear on the finger graphic to signal a partial registration has been made.

9 Ask the user to apply the same finger to the sensor of the fingerprint reader again. Again, redo the fingerprint until happy with it and then click the Verify button once more. This time the following should be displayed:



If the fingerprint image is strong enough, the software will display a score that is matched to the first fingerprint (the one being held at Stage 1).

The match score shows how successfully each fingerprint is being recognized by Sentinel.

Any score over 170 is very good. It is recommended that scores lower than 120 be rejected.

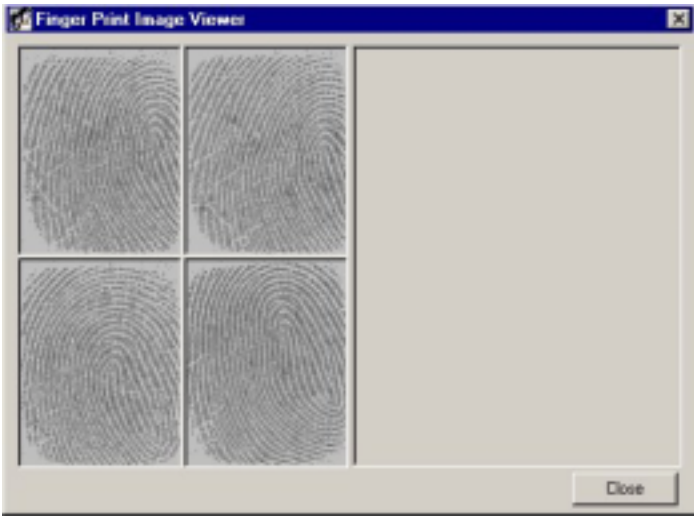
Click the **OK** button. If the score is unsatisfactory, retake the fingerprint and click *Verify* again until a successful match is achieved. If happy with the score - as in the previous example shown - then click on the **Stage 2** button to hold the image as the second fingerprint. The *Stage 3* button will become active.

The *Stage 1* button will remain active through all four stages so that the registration can be started again at any time if the fingerprints prove unsatisfactory (for example, if different parts of the finger are used - say the left side and then the right side - Sentinel will have difficulty matching the two images as they will be of different areas of the fingerprint).

10 Repeat the above procedure for **Stage 3** and **Stage 4**

After each stage check the finger diagram to ensure that the fingerprints are being matched to the correct finger.

At any time during each stage the fingerprints can be viewed by clicking on the **View Prints** button. An example of the *Fingerprint Image Viewer* window is shown below. If the quality of the images are not high, do not be afraid to start again.



Clicking the **Delete** button will clear all of the held images to start again with a clean slate. When the registration is complete, the red dot displayed on the finger graphic will turn blue.

11 Try two or three tests to check the access capability of the user by getting the user to provide additional fingerprints. Click the *Verify* button after each print appears on the *Fingerprint* page. The print should be identified with a matching score of consistently over 120. Routine scores below this will require the registration procedure to be repeated to improve recognition.

12 Repeat the registration procedure for each additional finger for that user (it is recommended that two or three fingers are registered for each user).

When finished click the **Stop** button.

13 Additional information for the user can be added by selecting the **Postal Address** page in the same window.

14 The user set-up procedure is now complete. Click the **OK** button to close the window saving all the information and the user's name will appear on the list in the *Users* window (for more general information about the *Users* window see the chapter *Setting Up Users for the ID Reader*).

The user can now be assigned access and security settings and associated to specific groups and specific ID readers in the normal way (see the chapters *Access and Security Settings* and *Managing Users for More than One ID Reader* to complete these user configuration procedures).

Important: Until the user has been assigned to a group (and that group is assigned to the device), they will not be able to use their fingerprints to gain access. Complete the full configuration procedures before attempting use.

15 Repeat the procedures detailed in this chapter to set up as many users as required. **Important:** See the next section for details on restarting the Sentinel Service or changing the device's server port back to default - which may or may not be required.

Restarting the Sentinel Service

Important: If the Stop Sentinel Service method has been used, When user registration is finished it is necessary to restart the service before the system can operate. How the service is started again will depend on the version of Windows the PC is running.

2000

From the **Start** menu select **Settings/Control Panel/ Administrative Tools/Services**. Select **Sentinel Service** from the list and click the **Action** button in the top left corner of the window. Select **Start**. On the list, the status of the service will now be listed as *Started*.

NT4 +

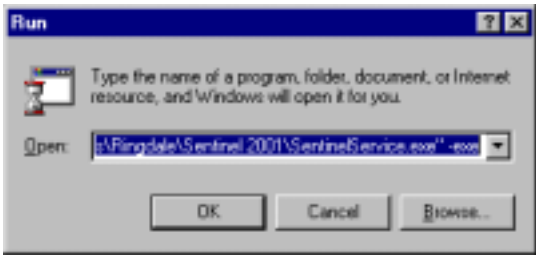
From the **Start** menu select **Settings/Control Panel/Services**. Select **Sentinel Service** from the list and click the **Start** button. On the list, the status of the service will now be listed as *Started*.

95/98/ME

Because these platforms do not run a *Services* feature the service is run as an executable program. Use the following procedure to restart the Sentinel Service:

1 Using *Windows Explorer*, navigate to the location of the Sentinel program files (normally C:\Program Files\Ringdale\ Sentinel 2001).

2 From the **Start** menu select **Run** and then drag the **Sentinel Service** details from Explorer into the *Run* dialog box as shown in the example below:



3 Scroll along to the end of the text thread and type 1 blank space, then **-exe** (no spaces between the minus and the letters) as shown in the example above.

The complete text should now read:

C:\Program Files\Ringdale\Sentinel 2001\SentinelService.exe -exe

4 Click the **OK** button and the Sentinel Service will be restarted (this can be checked by clicking the *Control*, *Alt* and *Delete* keys at the same time - Sentinel Service will be listed among the programs running).

Changing Back the Server Port for the Device

Important: If the changing of the server port method has been used, and when user registration is finished the fingerprint reader/access controller device needs to directly manage a door or Time and Attendance terminal, then the device needs to be reset to the previous server port.

If a dedicated desktop fingerprint reader and controller are being used for administration and registration purposes (and are not being used to directly manage a door or Time and Attendance terminal) then the server port should remain as set for registration.

Perform the following procedure ***Only*** if the device needs to directly manage access control as in the first of the above situations:

1 Click on the **Devices** icon at the top of the Sentinel software main window.

2 From the list of available devices select the controller required and click the **Properties** button to display the *Device Properties* window.

3 In the **Server Port** field, change the server port back to its original setting (normally 9103).

4 Click **OK** to save the change and exit the window.

The device should be prepared for access control once again.

Creating Reports for a Fingerprint Reader

This section needs to be read in conjunction with the general *Creating Reports* chapter later in the manual.

Important: The procedure for creating reports from a fingerprint reader is different from that for other readers. Because the fingerprint data is automatically stored on the server PC running Sentinel the log retrieval procedures detailed in the *Retrieving Information from the ID Reader/Access Controller* chapter do not need to be used. An access log report can be generated using this simple procedure:

1 Click on the **Reports** icon at the top of the Sentinel main window and ensure that the **Access Logs** option is selected from the drop-down menu at the top of the *Reports* window.

2 From the **From** drop-down calendar select the month and day that the report should start from. From the **To** drop-down calendar select the month and day where the report should finish.

To create a report for just one day set the same *From* and *To* dates.

3 From the list of devices, select the fingerprint reader/s required.

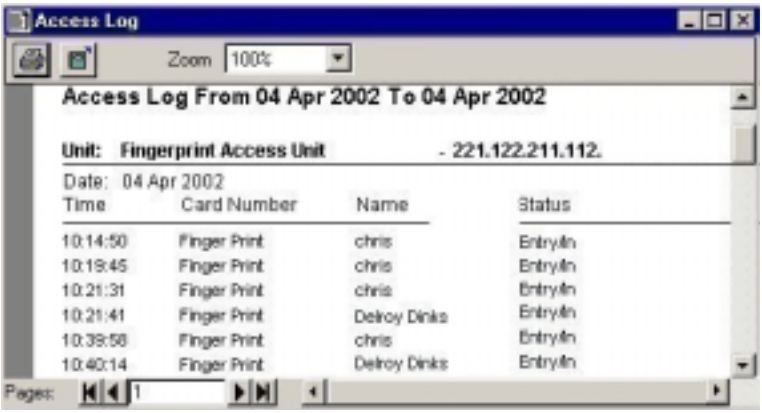
To select multiple devices hold down the **Control** key while selecting, or to select a block of devices together hold down the **Shift** key and select the devices at the top and bottom of the block.

Note: It is possible to generate an access log report of multiple devices which include both fingerprint readers and card/keypad readers. Just ensure that up-to-date logs have been retrieved for the non-fingerprint readers before generating the report.

4 To generate the report click the **Show Report** button.

Note: Be aware that if a device is heavily used creating a report with several devices can produce a large amount of data. The report might take a few moments to generate depending on the amount of data to be processed.

Below is an example of a fingerprint access log report:


Access Log
Zoom 100%
Access Log From 04 Apr 2002 To 04 Apr 2002
Unit: Fingerprint Access Unit - 221.122.211.112.
Date: 04 Apr 2002
Time Card Number Name Status
10:14:50 Finger Print chris EntryIn
10:19:45 Finger Print chris EntryIn
10:21:31 Finger Print chris EntryIn
10:21:41 Finger Print Delroy Dinks EntryIn
10:39:58 Finger Print chris EntryIn
10:40:14 Finger Print Delroy Dinks EntryIn
Pages: 1

Instead of the ID number that is normally displayed in the report, users set up for fingerprint access will be clearly shown.

There is no difference in the procedure to generate *Groups and Users* and *User Information* reports, though again, users registered for fingerprints will be displayed as such in place of an ID number.

Uploading Settings to the ID Reader/Access Controller

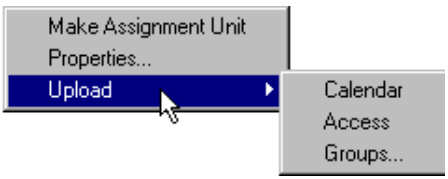
Once the users, groups and access and security settings are configured, or whenever any changes have been made to these settings, it is necessary to upload the information to the ID readers/access controllers themselves. ***This MUST be done for the new settings to take effect***. Upload the settings using one of the two following procedures:

a) Quick Upload Method to Single ID Reader/Access Controller

Use this method to upload the settings separately to one ID reader only.

1 In the main window of Sentinel, click on the **Devices** icon to display the list of ID readers/access controllers available.

2 Right click over the required device on the list to display the following pop-up window:



3 Select the **Upload** option to display the three additional options shown above.

(i) Selecting **Calendar** will upload the up-to-date calendar settings as currently configured in Sentinel to the ID reader required.

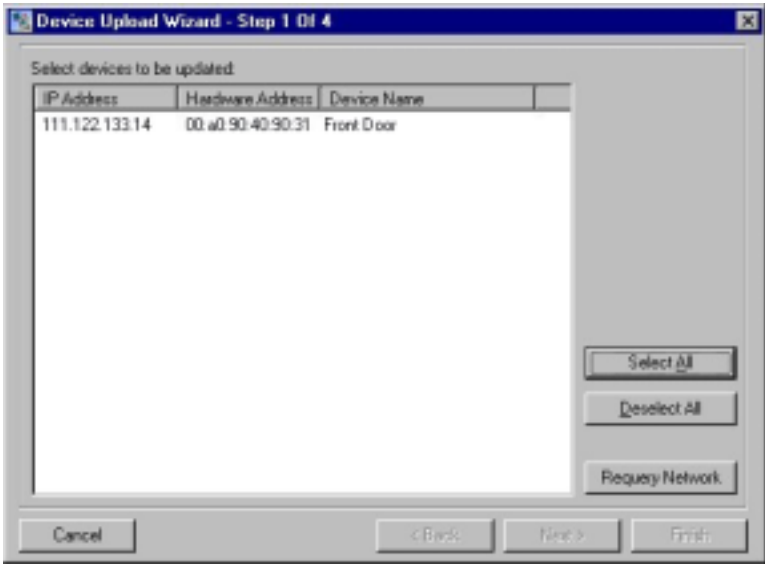
(ii) Selecting **Access** will upload the security access patterns for each day type as currently configured in Sentinel to the ID reader required.

(iii) To upload all details of groups associated to that particular device select **Groups**. All users set up in those groups will be assigned to that ID reader (if, for example, a user has been recently added or removed from one of these groups, uploading the revised groups will instantly make the ID reader up-to-date with the information from Sentinel).

b) Multiple Upload Method Using the Upload Wizard

For a more comprehensive and flexible method to update the ID readers/access controllers with the latest information use the Upload Wizard.

1 In the main window of Sentinel click on the **Upload** icon, as shown here. The first window of the wizard is shown below:



Here will be listed all of the ID readers/access controllers on the network - if all devices are not displayed here click on the **Requery Network** button.

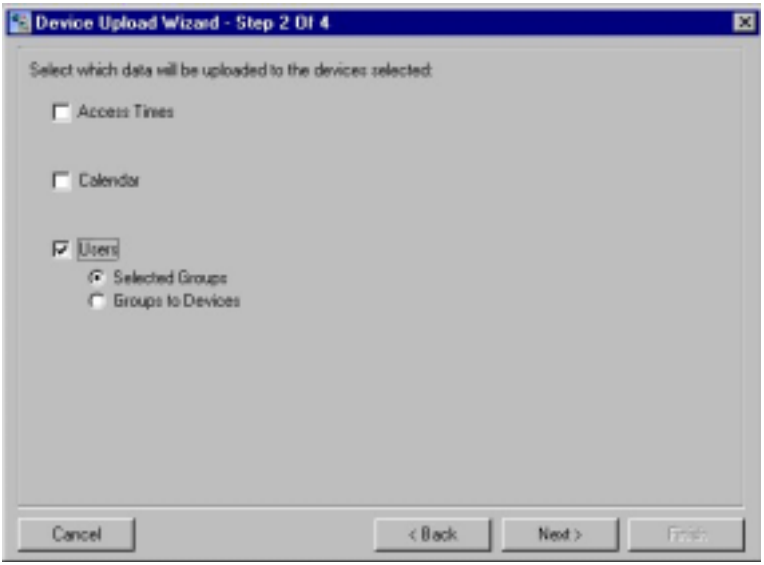
2 Select the device/s from the list that are to be uploaded with the new information .

To select multiple devices hold down the **Control** key while selecting, or to select a block of devices together hold down the **Shift** key and select the device at the top and bottom of the block.

To select all devices click on the **Select All** button.

Click on the **Deselect All** button to clear any incorrect selections that have been made and re-select devices.

3 When the devices required are selected click on the **Next** button to display the following window (**Note:** If a password has been set it will need to be entered at this point to continue with the wizard):



4 Select which data is to be uploaded (any combination of the three types can be uploaded at the same time).

Selecting **Access Times** will upload the security access patterns for each day type as currently configured in the software to the chosen ID readers/access controllers.

Selecting **Calendar** will upload the calendar settings for up to 360 days as currently configured in the software to the chosen ID readers/access controllers.

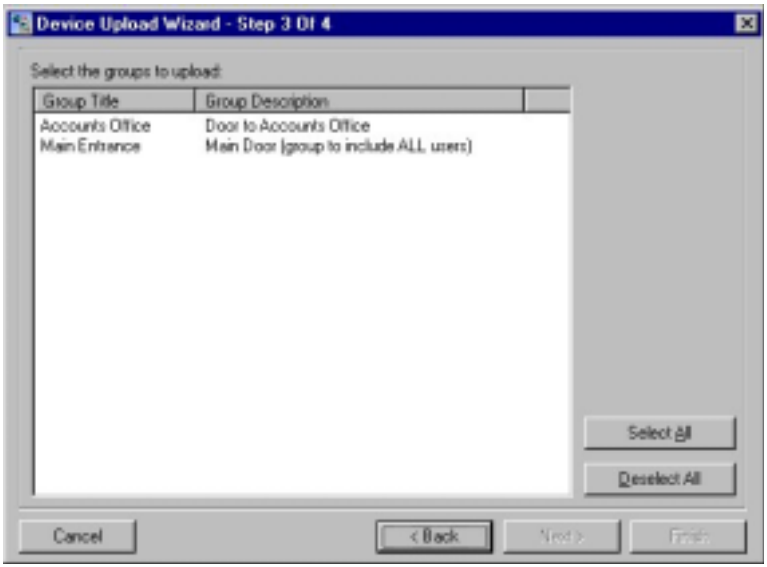
If either or both of these options are selected ***without*** the *Users* option, then click **Next** to skip straight to the *Step 4* wizard window.

Selecting **Users** will provide a choice of two options:

a) Choosing **Groups to Devices** will upload all associated user groups and their details (including security levels) as currently configured in the software to the ID readers/ access controllers that have been selected.

If this option is selected click the **Next** button to skip straight to the *Step 4* wizard window.

b) Choosing the **Selected Groups** option and clicking the **Next** button will display the following *Step 3* wizard window:



This window will display the list of all user groups currently available in Sentinel. From the list select the user group/s to be uploaded to the chosen ID readers/access controllers.

To select multiple groups hold down the **Control** key while selecting, or to select a block of groups together hold down the **Shift** key and select the group at the top and bottom of the block.

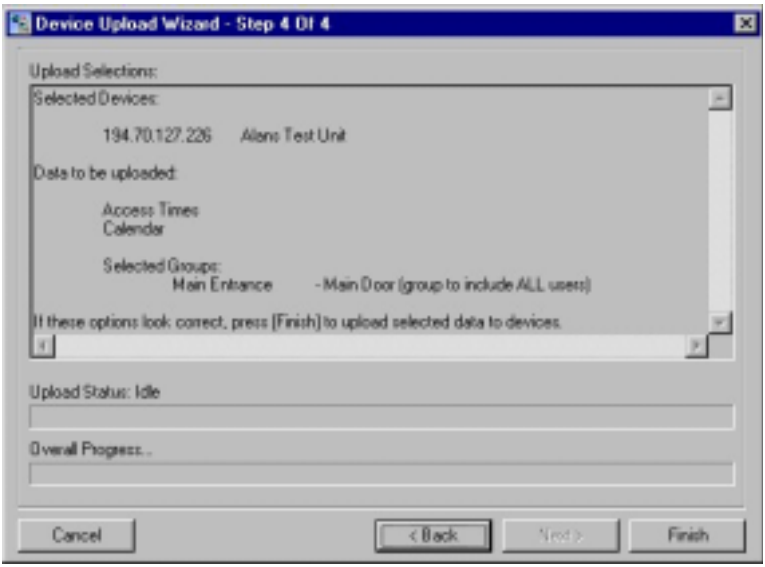
To select all groups click on the **Select All** button.

Click on the **Deselect All** button to clear any incorrect selections that have been made and re-select the groups.

Important

Care needs to be taken with this procedure - using the *Select All* button will assign every group to the selected ID readers/access controllers and give all users access through those devices. Similarly, selecting the wrong group by mistake will give that group access through the device whether the device is associated to the group or not.

When the group/s have been selected as required click the **Next** button to display the *Step 4* wizard window shown below:



5 This window allows the data that is about to be uploaded to be checked and confirmed. Ensure the information is correct and that the selected device/s are correct.

When happy, click the **Finish** button. Two graphics at the bottom of the screen allow the upload process to be monitored.

When the upload is complete the following dialog box will be displayed:

Report - Upload Process
Some information about the upload process:
Uploaded Access Times to: 194.70.127.226
Uploaded Groups to: 194.70.127.226
Close

This will inform if the upload was successful. Click **Close** to finish.

Door Strike and Bolt Control Options

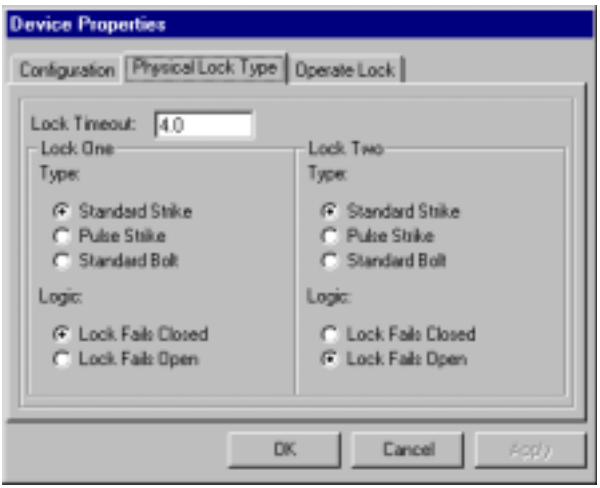
Sentinel gives the ability to remotely control the set-up and operation of a door strike or bolt if the ID reader/access controller is managing this kind of device (this option will not be present if the ID reader/access controller is being used to manage a time and attendance terminal - see the separate chapter for details of the different options available with this feature).

The correct door strike or bolt type MUST be set in sentinel before attempting to use the device.

Access the control options as follows:

1 In the Sentinel main window, click on the **Devices** icon to display a list of the available devices on the network.

2 From the list, select the device that is managing the door strike or bolt and open the property pages. Select the **Physical Lock Type** tab to display the following page (**important note:** this page has the capability to manage two different locks. This is for use with the *Duplo* version of the access controller which can manage two locks simultaneously - or alternatively two ID readers on one lock. If the *Solo* version is being used only the **Lock One** field is to be used):



3 In the **Lock Timeout** box enter the amount of time in seconds that the lock will be 'live' for once activated by a successful ID (for example, a five second timeout would give a user five seconds to access the door after ID recognition before the door would lock again).

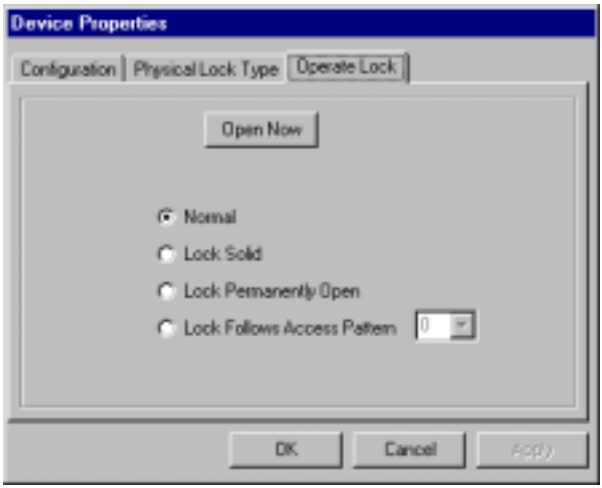
4 In the *Type* field, select the strike or bolt type that is connected to the access controller. If a strike is connected, ensure that the **Standard Strike** option is chosen.

Only select the **Pulse Strike** option if told to do so by a member of the Ringdale technical support team.

If a bolt is connected to the access controller, select the **Standard Bolt** option.

5 If a Ringdale brand strike is connected the **Logic** field will become active. Select whether the strike is of the **Lock Fails Closed (PTO)** type or the **Lock Fails Open (PTL)** type (this will be detailed on the strike itself).

6 Click **Apply** to save the settings and then click on the **Operate Lock** tab to display the following page:



This page provides the ability to remotely operate the lock or to override the current operation settings.

Set the following features as required:

Open Now
This button gives the ability to remotely open the door using the Sentinel software - directly from the workstation.

Normal Operation
Select this option for the system to operate to the access and security settings as uploaded to the ID reader/access controller.

Lock Solid
Select this option to keep the lock permanently closed.

Lock Permanently Open
Select this option to keep the lock permanently open.

Lock Follows Access Pattern
This option allows greater flexibility in the strike/bolt management by allowing the access controller to be associated with one of the security access levels set up in the *Access Times* Window (see the *Access and Security Settings* chapter). Once associated to a specific level, general access can be provided for a specified period, while restricted access is allowed outside the period. Following is a typical example of this feature in operation:

> Store XYZ has an ID reader by its main door. The store opens from 10:00 am to 4:00 pm. During this time the door needs to be open for customers to come and go, so no ID is needed at this time to gain entry.
>
> Access Level 5 is set at 10:00 am till 4:00 pm. The door strike is set to follow this access pattern. Unrestricted access is granted through the main door for this period.
>
> Before 10:00 am and after 4:00 pm, an ID will be needed to gain access through the door and the door will lock again after use, enabling staff to enter.
>
> The period the staff can enter will still be regulated by the access level they have been assigned. For example, general staff will only be able to enter

between 8:30 am and 6:00 pm, managers will have 24 hour access.

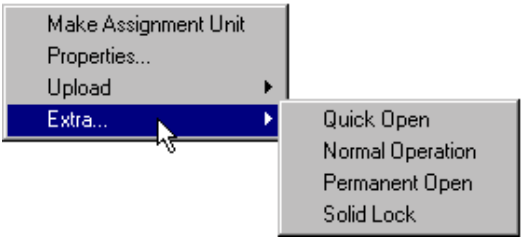
The door strike will automatically activate at 4:00 pm, so an ID will be needed to gain access from this time. However, ***the lock will not automatically deactivate at 10:00 am***. An ID will be needed to gain entry the first time after 10:00 am to ensure complete security.

Set the strike to follow the access pattern by selecting the level required from the drop-down list after selecting the **Lock Follows Access Pattern** option.

7 Click **Apply** to save any settings made on this page, or **OK** to exit the property pages saving any changes. To exit without saving any settings that have been made on the page click on **Cancel**.

Quick Select Options

The following features described above are available as quick select options by right clicking over the required device on the list in the *Devices* window to display the pop-up menu shown here:



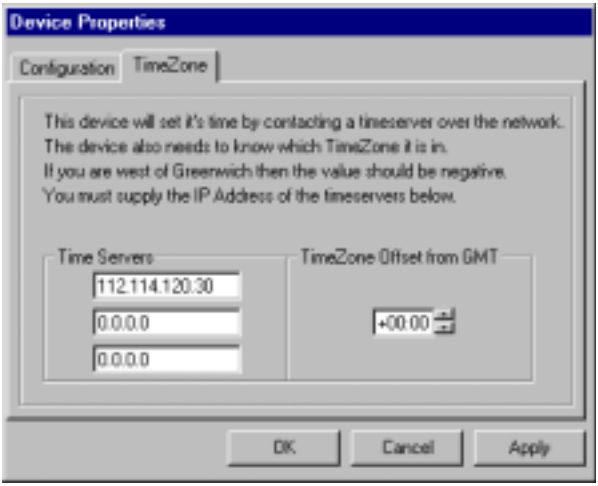
Select the **Extra** option to display the secondary menu. Select the option as required.

Time and Attendance Terminal

If the ID reader/access controller is being used to manage a time and attendance terminal, an additional configuration page will be present instead of the door strike and bolt control options. This will need to be configured to ensure accurate time keeping. To access the page:

1 In the Sentinel main window, click on the **Devices** icon to display a list of the available devices on the network.

2 From the list, select the device that is managing the time and attendance terminal and open the property pages. Select the **Timezone** tab to display the following page



3 Enter up to three IP addresses of **Time Servers** in the boxes provided. The device will set its time by contacting the first address. If the first address fails to respond the second address will be contacted. The third address will only be contacted if the first two time servers cannot be contacted. This can ensure a high level of reliability for the time signal.

4 All time servers work to GMT. In the **Time Zone Offset from GMT** field it is necessary to set the time zone that the terminal is in. Zones east of Greenwich are ahead of GMT, zones west are behind GMT. Click **Apply/OK** to save the information.

Retrieving Information from the ID Reader/Access Controller

Sentinel can be set to retrieve the ID reader/access controller data logs to allow each device's use to be monitored. Once retrieved, the information can also be used to create reports (see the separate chapter *Creating Reports* for more details of this). The information is stored in either a Microsoft Access or SQL database depending on the option chosen on installation (see the chapter *First Time Set-Up Procedure* for details on setting up the database).

Retrieval can be set to run automatically so that Sentinel downloads the current data from any or all ID readers/access controllers every minute (depending on the level of network traffic), ensuring that the software always has the latest information.

However, if there are a lot of devices on the network this can create a large amount of network traffic so it is recommended that this facility is only used for multiple devices when really necessary. Alternatively the information can be retrieved manually for each device as and when required. Following are details for using both methods:

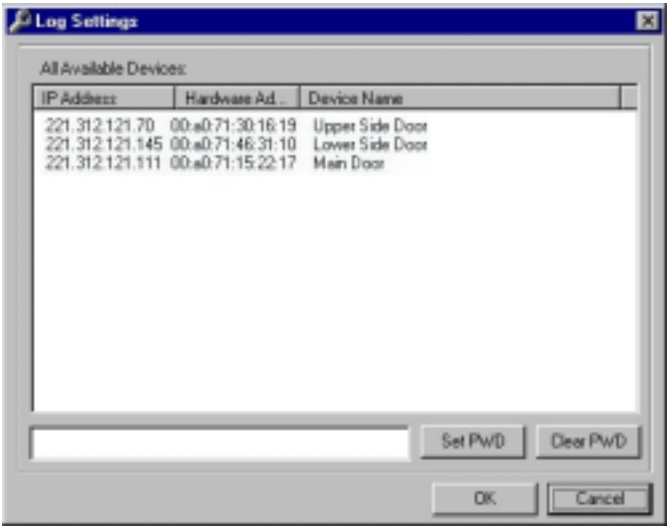
Automatic Log Retrieval

To set up an ID reader/access controller to automatically download it's log use the following procedure:

Note: Ensure that the database is correctly set up and that the Sentinel Logger is *Enabled* before starting (see the chapter *First Time Set-Up Procedure* for details).

1 In the Sentinel main window, select the **Log Settings** option from the *Tools* drop-down menu to display the window shown following.

2 From the list select the device/s required. To select multiple devices hold down the **Control** key while selecting, or to select a block of devices together hold down the **Shift** key and select the device at the top and bottom of the block.



3 Click **OK** and those devices highlighted will now be set to automatically download the log to the database.

To stop the automatic download at any time open the above window again. All devices currently selected for downloading will be highlighted. Click in a blank space to remove all the selections. Make any new selections as required.

Important

This window also offers an alternative place to set up a password for the devices to restrict access to change any data within Sentinel (the device property pages provide the same option). It is strongly recommended that a password is used.

Before creating a password here, ensure that a password has not been previously created when the device was originally configured to the network.

To set a password in this window select the devices from the list and enter the word into the text box at the bottom of the window. Click the **Set PWD** button to apply. Select the devices from the list and click the **Clear PWD** button to remove the password if required.

Important Note: To use the password feature with automatic logging all devices need to be given the same password.

Manual Log Retrieval

To manually retrieve the log from one ID reader/access controller use the following procedure:

Note: Ensure that the database is correctly set up before starting (see the chapter *First Time Set-Up Procedure* for details).

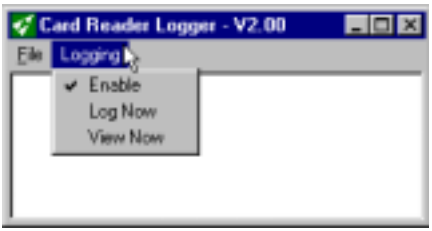
1 In the Sentinel main window, select the **Log Settings** option from the *Tools* drop-down menu to display the window shown previously.

2 From the list select the device from which the data is to be downloaded and ensure no other device is selected.

3 Click **OK** to exit saving the selection.

Please note the details concerning passwords as explained in the *Automatic Log Retrieval* section above, except if manual downloading is to be used devices do not have to have the same password as each other.

4 Double click on the **Ringdale** icon located in the bottom right corner of the screen, as shown here. This will display the Sentinel Logger window as shown below:



5 In the *Logging* drop-down menu, ensure that the Sentinel Logger is ***Not*** *Enabled* by ***Unticking*** it if necessary.

6 From the *Logging* drop-down menu select **Log Now** and the log will be downloaded to the Sentinel database. Click the *Minimize* button to exit.

Viewing a Log

The current log from any ID reader/access controller can be viewed before/instead of downloading the data using the following procedure:

1 In the Sentinel main window, select the **Log Settings** option from the *Tools* drop-down menu to display the window shown previously.

2 From the list select the device/s for which the log is to be viewed and ensure no other device/s are selected.

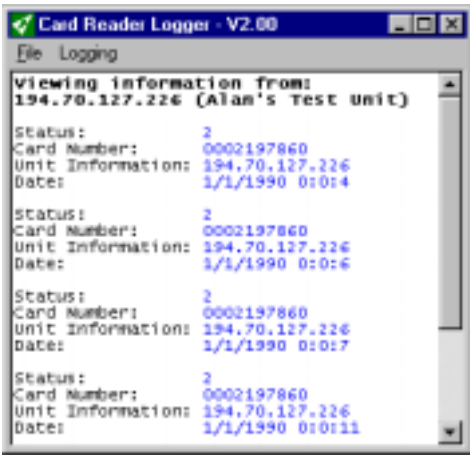
3 Click **OK** to exit saving the selection.

Please note the details concerning passwords as explained in the previous sections of this chapter.

4 Double click on the **Ringdale** icon located in the bottom right corner of the screen, as shown here. This will display the Sentinel Logger window as shown previously.

5 From the *Logging* drop down menu ensure that the **Enable** option is ***Unticked***.

6 From the *Logging* drop down menu select **View Now**. The current log for the device/s selected will be displayed.



A typical example is shown here

Click the ***Minimize*** button to exit.

The following data will be displayed for each event that has been logged by the selected ID readers/access controllers.

Card Number
The card/ID number of the user will be displayed here.

DateTime
The time and date that the ID was used will be displayed here.

Unit
The IP address of the ID reader/controller will be displayed here.

Status
The flag code will be displayed here, please see the section following for details of the flagging codes.

Flag Codes

As shown in the *Viewing a Remote Log* section, Sentinel uses a flagging system to register ID use. The log will display a number each time an ID is used - this will be listed under the *Status* heading. Below is a list of what each number represents - taking into account that the reader/controller can be used for more than one purpose (*Access Control* or *Time and Attendance*):

1 Entry/In

2 Not Recognized/Out

3 Not Allowed/Error

129 Already In

130 Already Out

The words used here will be displayed on any *Access Log* reports that are generated (see the following chapter for details on this).

Note: the numbers 129 and 130 are flags only used when the reader/controller is set up for time and attendance.

Creating Reports

Once the data from each ID reader/access controller has been downloaded to the database (see the chapter *Retrieving Information from the ID Reader/Access Controller* for details on this) reports can be generated.

Three types of reports can be created:

Access Logs This option allows the generation of reports based on the information downloaded from each device, including when access was granted, who to, which device etc.

Groups and Users This option allows a list of the existing groups and the users assigned to those groups to be printed out.

User Information This option allows a list of users and their full details to be printed out.

To access the report creation features, click on the **Reports** icon at the top of the Sentinel main window as shown here.

From the **Please Select a Report** drop-down menu at the top of the displayed window, select the option for the type of report to be generated.

Following is a section detailing the procedure for using each option. Select as required:

Note: ***The Fingerprint Reader Option does not require the retrieval of the access log to generate a report. If using this option please see the separate chapter before attempting to create a report.***

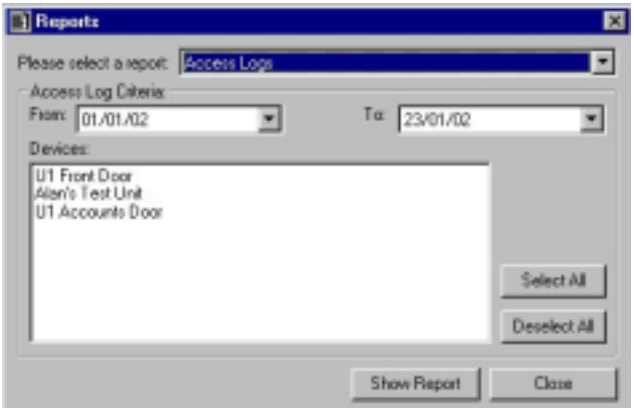
Access Logs

To create an *Access Logs* report it is necessary to have retrieved the data from the ID reader/access controller. If Sentinel has been set to automatically download the log from

the device this procedure will already have been completed. If not, the log will have to be downloaded manually. Both procedures are explained in the previous chapter.

To create an *Access Logs* report follow these steps:

1 Ensure that the **Access Logs** option is selected from the drop-down menu at the top of the *Reports* window (this is the default option, so should be displayed automatically). An example of the window is shown following, with a calendar option in the top half and a list of all the devices configured to Sentinel in the bottom half.



2 From the **From** drop-down calendar select the month and day that the report should start from.

3 From the **To** drop-down calendar select the month and day where the report should finish.

To create a report for just one day set the same *From* and *To* dates.

4 From the list of devices, select the ID reader/access controller whose log should be used to create the report.

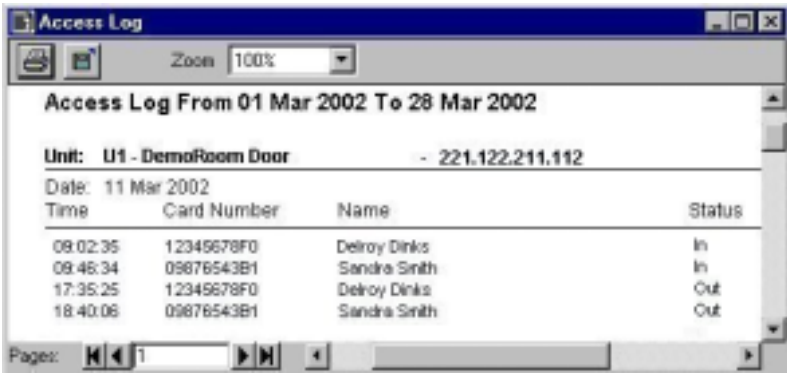
To select multiple devices hold down the **Control** key while selecting, or to select a block of devices together hold down the **Shift** key and select the devices at the top and bottom of the block.

To select all devices click on the **Select All** button. Click on the **Deselect All** button to clear any incorrect selections that have been made and re-select the device/s.

5 To generate the report click the **Show Report** button.

Note: Be aware that if a device is heavily used creating a report with several devices can produce a large amount of data. The report might take a few moments to generate depending on the amount of data to be processed.

Below is an example of an *Access Log* report (**Note:** If a fingerprint reader is being used this will create a slightly different report. See the chapter Fingerprint Reader Option for details of this):


Access Log
Zoom 100%
Access Log From 01 Mar 2002 To 28 Mar 2002
Unit: U1 - DemoRoom Door - 221.122.211.112
Date: 11 Mar 2002
Time Card Number Name Status
09:02:35 12345678F0 Delroy Dinks In
09:48:34 09876543B1 Sandra Smith In
17:35:25 12345678F0 Delroy Dinks Out
18:40:06 09876543B1 Sandra Smith Out
Pages: 1

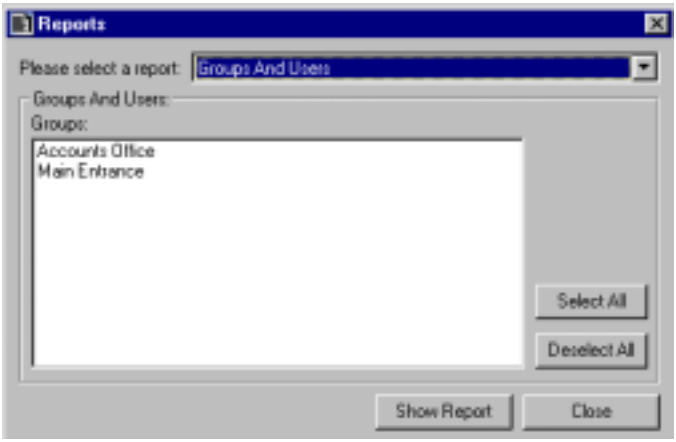
The report will display the ID number, the time it was used and the name of the ID holder together with a status reading for the ID (this will depend on the flag number generated by the reader when it read the ID - see the *Flag Codes* section of the *Retrieving Information from the ID Reader/Access Controller* chapter for details). In this simple example the report is for a Time and Attendance terminal - two users have clocked in and clocked out, the status acknowledges this. If access had been denied for a user or the reader had been unable to identify the ID, this would also be displayed.

The toolbar across the top of the report offers the ability to zoom in to specific parts of the report if required and also provides an export and print function (see later in the chapter for full details of this).

Groups and Users

To create a *Groups and Users* report follow these steps:

1 Select the **Groups and Users** option from the drop-down menu at the top of the *Reports* window to show the following page:



2 A list of all groups that have been created in Sentinel will be displayed. Select the group/s required to be in the report.

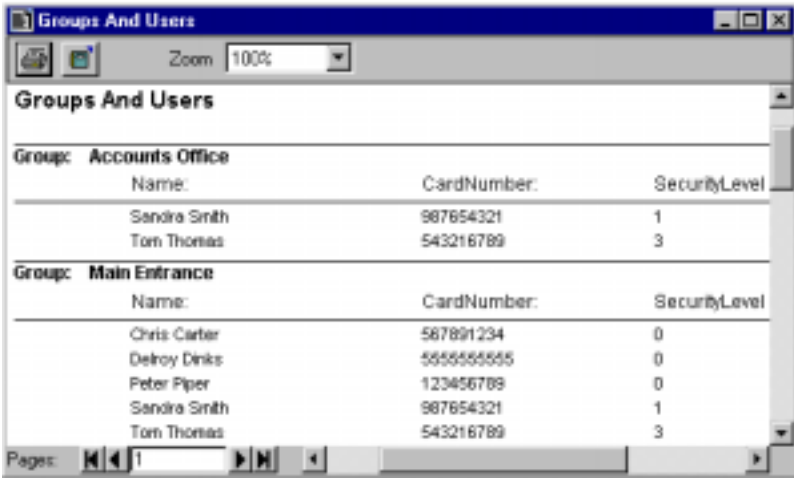
To select multiple groups hold down the **Control** key while selecting, or to select a block of groups together hold down the **Shift** key and select the group at the top and bottom of the block.

To select all groups click on the **Select All** button.

Click on the **Deselect All** button to clear any incorrect selections that have been made and re-select the groups.

3 To generate the report click the **Show Report** button.

Following is an example of the *Groups and Users* report that will be displayed:

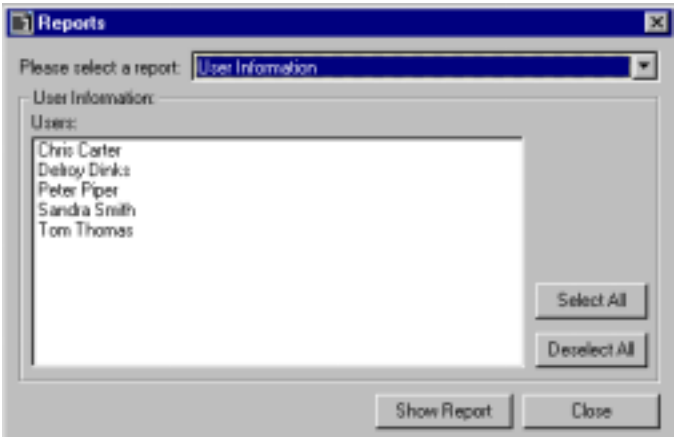


Each group selected will be displayed in alphabetical order with a list of the users assigned to that group.

User Information

To create a *User Information* report follow these steps:

1 Select the **User Information** option from the drop-down menu at the top of the *Reports* window to show the following page:



2 A list of all users that have been set up in Sentinel will be displayed. Select the users required to be in the report.

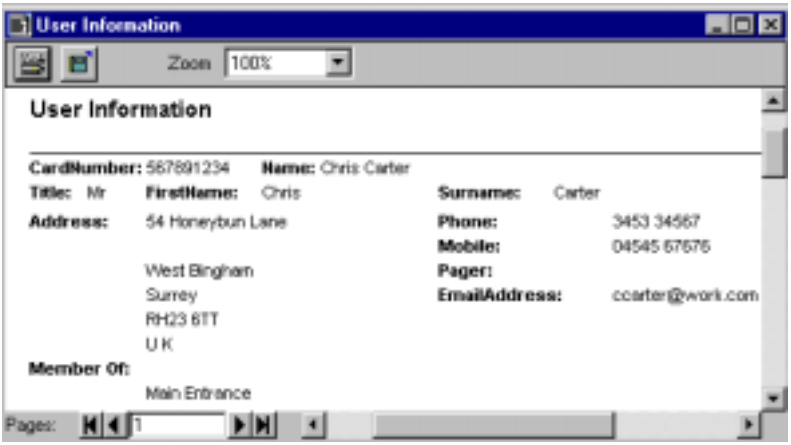
To select multiple users hold down the **Control** key while selecting, or to select a block of users together hold down the **Shift** key and select the user at the top and bottom of the block.

To select all users click on the **Select All** button.

Click on the **Deselect All** button to clear any incorrect selections that have been made and re-select the users required.

3 To generate the report click the **Show Report** button.

Following is an example of the *User Information* report that will be displayed:



All the details held in Sentinel about each selected user will be displayed, including ID number and a list of groups to which they are assigned.

Printing and Exporting Reports

All three types of reports can be printed or exported and saved as a file if required:

To print a report simply click on the **Print** icon in the top right corner of the window. The regular Windows printer options will appear. Print all or part of the report as required.

To export a report click on the **Export** icon (located next to the *Print* icon). Navigate to the location where the file is to be stored, name the file and save as either a text (txt) or HTML (html) document.

Personnel Monitor Option

If the Personnel Monitor Option has been installed, the set-up procedures detailed here will need to be completed to get the system functioning. This option provides for a display of the personnel who are currently logged on.

An example of a typical set-up is as follows:

Company A has a secure area with restricted access. In order to establish who is present in the restricted area they have installed the Personnel Monitor Option. Each user to be registered to the restricted area has their photograph taken and the photo is loaded and stored in Sentinel (it is not necessary to use a photograph for the system to work).

Every time the user is logged on as having entered the restricted area, Sentinel will send their name and photograph to a dedicated, rugged PC with a monitor attached. This PC will also be running the Sentinel software

All users currently logged on will be displayed on the monitor so those outside the restricted area can see at a glance who is inside the restricted area. When the user logs out, their name/photograph will be removed from the display.

Use the following procedure to set up Sentinel for the Personnel Monitor Option:

Adding a Photograph to a User's Details (Recommended)

Note: It is not necessary to add a photograph to use this feature.

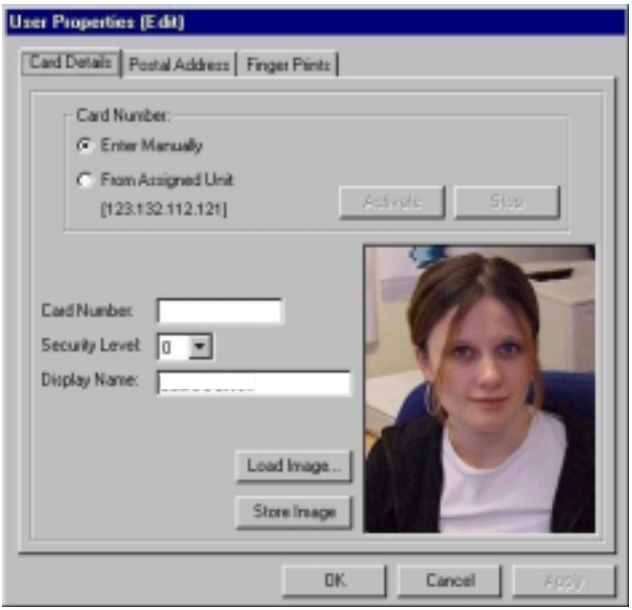
1 In the Sentinel server main window, click on the **Users** icon to display a list of the registered users.

2 Select the user required from the list and click the **Edit** button to display the *User Properties* window (to set up a new user see the chapter *Setting Up Users for the ID Reader*). Ensure that the **Card Details** tab is selected:

3 Click the **Load Image** button and browse to the location of the file. Click **OK** and the photo will be displayed in the image box.

4 If the photo is correct click the **Store Image** button to store the photo in the database.

An example of user details with a photo is shown below:



5 Repeat procedure for as many users as required.

6 Click **OK** to exit.

The photos can be viewed at any time by opening the *User Properties* window of each user.

Setting up Sentinel on the Monitor PC

The dedicated, rugged PC that will provide the monitor display is supplied with the Sentinel software pre-installed (if this is not the case see the *Sentinel Installation* chapter of this manual and install the software).

See also the *First Time Set-Up Procedure* chapter. ***These instructions must be completed for the monitor PC, taking into account the following database set-up differences***.

Microsoft Access
Instead of creating a new database for the monitor PC, the Sentinel software needs to be linked to the ***Sentinel Server PC database*** (if unsure about the location of this database, it will be detailed in the *Database Settings* option of the *Tools* menu of the Sentinel main window on the server PC).

In the *Database Settings* window of the Monitor PC, instead of clicking the *New* button, click the **Browse** button and navigate across the network to the ***Sentinel Server's Database***. Continue with the instructions as detailed in the *First Time Set-Up Procedure* to finish.

SQL Server
The SQL configuration for the monitor PC will need to be the ***same*** as that for the ***Sentinel Server PC*** (if unsure about the configuration of this database, it will be detailed in the *Database Settings* option of the *Tools* menu of the Sentinel main window on the server PC).

Once the set-up procedure is completed, the *Sentinel Monitor* application needs to be running.

Starting the Sentinel Monitor Application
From the **Start** menu select the following path:

Programs/Ringdale/Sentinel 2001/Sentinel Monitor

or alternatively, locate the application in *Windows Explorer* (it will be located with the other Sentinel program files), normal location:

C:\Program Files\Ringdale\Sentinel 2001\Sentinel2001AT.exe

Initially, the monitor should be displaying an empty black screen until an ID reader/access controller is associated to the monitor PC and users start to log on.

This completes the set-up of Sentinel on the monitor PC.

Note: To return the monitor PC to the *Windows* environment press the **Esc** key.

Important: It is recommended that the Sentinel Monitor application (Sentinel2001AT.exe) is set to automatically start up when the PC is booted - The monitor PC is designed to log itself on automatically when re-booting and having the application auto starting will minimize any interruption of service.

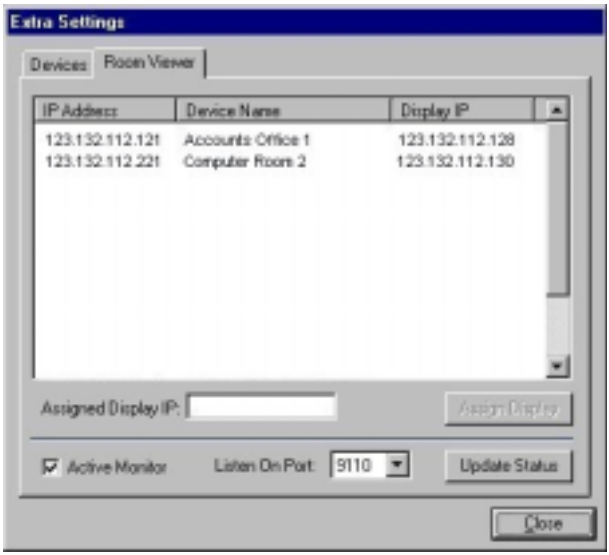
Associating the Monitor to an ID Reader/Access Controller

All users that are to be included in the Personnel Monitor will need to be in a group that is assigned to the ID reader/access controller that is being monitored - or if applicable more than one (see the chapter *Assigning Users to a Group and Managing Users for More than One ID Reader* for details on this).

It is then necessary to associate that ID reader/access controller with the monitor PC. Use the following procedure on the ***Sentinel Server PC*** for this:

1 In the Sentinel main window, select the **Extra Settings** option from the **Tools** menu.

Select the **Room Viewer** tab. The following window will be displayed:



All the ID reader/access controller devices available will be listed (**Note:** Though in the example shown the *Display IP* column is filled, on first opening this heading will be empty).

2 Select the device required from the list - the one whose access control is to be monitored.

3 In the **Assigned Display IP** box enter the IP address for the **Monitor PC**. Click the **Assign Display** button and the IP address will be associated with the selected device and be shown in the *Display IP* column.

4 By default the **Active Monitor** box is ticked. It is recommended that this option is kept this way. Deselecting this option will stop the monitor PC communicating with the Sentinel server.

5 If the *Active Monitor* box has been unticked, clicking the **Update Status** button will allow the monitor to receive and display the latest personnel log on status.

6 The **Listen On Port** drop-down box allows the port number being used to communicate between the Sentinel server and the monitor PC to be changed if required (this should only need to be changed if the default port number is already being used by something else).

Note: If the port number is changed it will be necessary to restart the Sentinel Monitor application on the monitor PC to allow the monitor to pick up the new port number setting.

7 When set-up is completed as required, click the **Close** button to exit the window.

The Personnel Monitor Option is now ready for use.

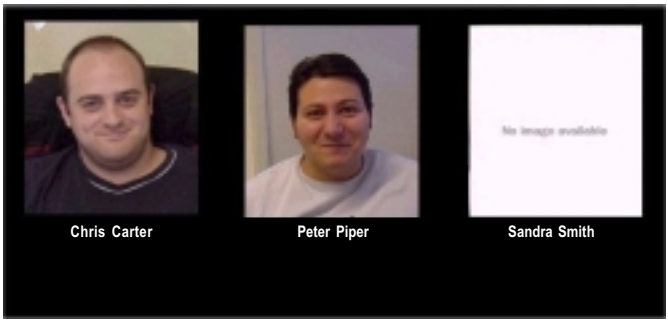
The Monitor Screen Display

When a user from a group assigned to the ID reader/access controller that is associated to the monitor PC logs on, their name and picture will appear on the monitor screen. When they log off, their name and picture will disappear. Thus, from looking at the screen it can be established who is present and who is not.

The photos will be displayed on a black background, and will automatically resize themselves to ensure all are visible on the screen at any time.

If there is no photo available for the user, an empty box will be displayed with the user's name underneath.

Below is a part view of a screen giving examples of users logged on both with and without photos



Uninstalling the Sentinel Software

Note: It is recommended that older versions of Sentinel be uninstalled before a new version is installed. If using the Access database option the data held by the old version of Sentinel will not be lost as this is stored in a separate .mdb Microsoft Access file - ensure that the new version of Sentinel is directed to this file to hold onto the data (or to the SQL database if that option is being used).

To uninstall the Sentinel software follow this procedure:

1 Double click on the green Ringdale icon in the bottom right corner of the screen to display the Sentinel Logger window.

2 From the **Logging** menu ensure that the **Enable** option is ***Un****ticked* and close the Logger window. A message will appear asking if the Logger program should be stopped. Click the **Yes** button.

3 The Sentinel Service will need to be stopped before the uninstall can take place. How the Sentinel Service is stopped will depend on the version of Windows the PC is running.

2000

From the **Start** menu select **Settings/Control Panel/ Administrative Tools/Services**. Select **Sentinel Service** from the list and click the **Action** button in the top left corner of the window. Select **Stop**. On the list, the status of the service will no longer be listed as *Started*.

NT4 +

From the **Start** menu select **Settings/Control Panel/Services**. Select **Sentinel Service** from the list and click the **Stop** button. On the list, the status of the service will no longer be listed as *Started*.

95/98/ME

Because these platforms do not run a *Services* feature the service is run as an executable program. To stop the service running press **Control**, **Alt** and **Delete** together ***Once*** to display the *Task Manager*. Select **Sentinelservice** from the list and click the **End Task** button. The service will be stopped.

4 From the **Start** menu select **Settings/Control Panel/Add/ Remove Programs** and select **Sentinel 2001** from the list. Click on the **Add/Remove** button and the program will be removed from your PC (the **.mdb** file will not be removed).

If the uninstall is a preliminary to the installation of a new version of Sentinel, it will be necessary to re-boot the PC.

Ringdale Ltd
56 Victoria Road
Burgess Hill
West Sussex
RH15 9LR
United Kingdom

Freephone: 0800 214503
Tel: +44 (0) 1444 871349
Fax: +44 (0) 1444 870228

Ringdale GmbH
Cochemer Straße 12-14
D-68309 Mannheim
Germany

Freephone: 0800 - 8251880
Tel: +49 (0) 621 7186-0
Fax: +49 (0) 621 7186-20

Ringdale Inc
101 Halmar Cove
Georgetown, Texas 78628
USA

Freephone: 888 288 9080
Tel: +1 512 288 9080
Fax: +1 512 288 7210

Rikei Corporation
1-26-2, Nishi-Shinjuku, Shinjuku-ku
Tokyo 163-05
Japan

Tel: +81-3-3345-2189
Fax: +81-3-3344-3949

Website: http://www.ringdale.com